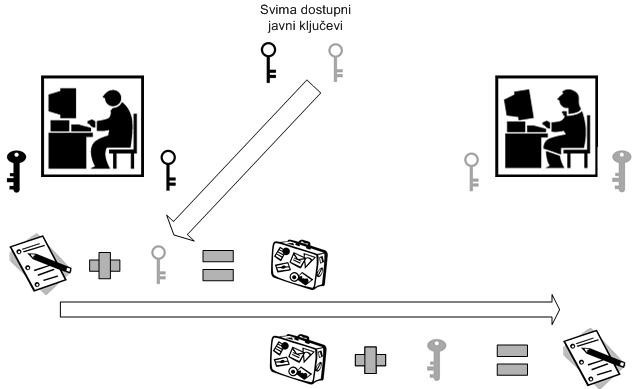
## Asimetrična kriptografija

Utemeljitelji asimetrične kriptografije su W. Diffie i E. Hellman koji su 1976. godine opisali ideju kriptografije koja se temelji na dva ključa, privatnom i javnom ključu. Razlik asimetričnih i asimetričnih algoritama je u tome što simetrični algoritmi koriste isti ključ za kriptiranje i dekriptiranje dok asimetrični algoritmi koriste različite ključeve za kriptiranje I dekriptiranje. Informacije kriptirane javnim ključem mogu se dekriptirati samo privatnim ključem odnosno to može samo osoba koja je vlasnik tajnog asimetričnog ključa. Osim toga kriptiranje javnim a dekriptiranje tajnim ključem pokazalo se također kao odlično svojstvo i omogućava digitalno potpisivanje informacija gdje potpis može biti provjeren javnim ključem od bilo koga.Ključevi trebaju biti povezani jednosmjernom funkcijom. Odnosno ne smije se moći izračunati privatni ključ iz javnog ključa ili se barem ne smije moći izračunati u razumnom vremenu.Asimetrični kriptosistemi zasnivaju se na određenim svojstvima brojeva koji spadaju u teoriju brojeva.Pri kriptiranju se razgovjetni tekst kodira kao niz prirodnih brojeva koji se odabranom funkcijom kriptiranja i ključem kriptiranja *Ke* preračunavaju u niz brojeva kriptiranog teksta.Funkcija kriptiranja mora biti takva da iz niza brojeva kriptiranog teksta napadač samo s velikim naporima može odrediti izvorni niz brojeva.Međutim,poznavajući ključ dekriptiranja *Kd* omogućuje lako izračunavanje izvornog niza brojeva. Asimetrično kriptiranje,slika 3.2,predstavlja složeniji vid zaštite podataka. Za njegovu realizaciju potrebna su nam dva ključa kod svakog od sugovornika. Jedan ključ je dostupan svima preko javnih kataloga ili imenika, te se zbog te osobine i naziva *javni ključ*. Drugi ključ poznat je samo vlasniku i naziva se *tajnim*.Iako su različiti, ključevi su međusobno povezani određenim transformacijama. Ako ponovo pogledamo prethodni primjer, sada je situacija bitno drukčija:Pero šifrira poruku Ani upotrebom njenog javnog ključa koji je svima dostupan. Mogao ga je dobiti putem email-a, preuzeti sa njenog Web sajta i sl. Bilo tko tko presretne ovu komunikaciju i pored toga što poznaje Anin javni ključ nemože otkriti sadržaj poruke. Poruku može dešifrirati samo Ana korištenjem svog tajnog ključa.Na ovaj način poruka je zaštićena od trećeg lica koji je prilikom presretanja šifrirane poruke onemogućen u

njenom dešifriranju jer mu je za to poreban ključ kojeg strogo u tajnosti čuva ciljni sugovornik. Glavne mane ovog kriptiranja su njegova sporost I neprikladnost za šifriranje velikih količina podataka.



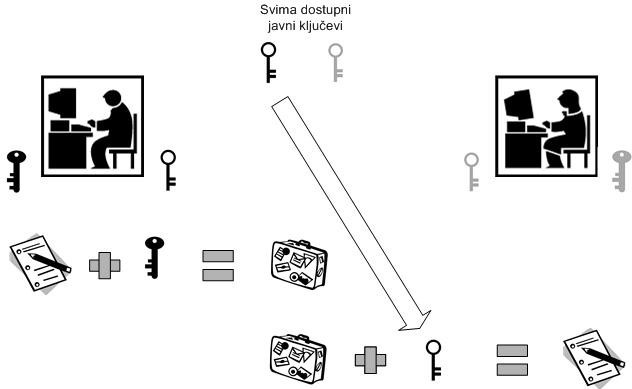
Često korišteni asimetrični algoritmi: RSA (Rivest-Shamir-Adleman), Diffie-Hellman, te ostali: ElGamal, Rabin, Eliptic Curves.Ovaj sistem predstavlja rješenje za prva dva uslova koja smo na početku ovog teksta postavili - zaštitu tajnosti informacija i očuvanje njihovog integriteta.Ostaje otvoreno pitanje kako da Ana bude sigurna da je poruku koju je primila uistinu poslao Pero.Osiguravanje autentičnosti informacija tj. definiranje i provjera identiteta pošiljaoca postiže se upotrebom digitalnih potpisa i digitalnih certifikata.

## 1.Digitalni potpis

Tehnologija digitalnog potpisa također koristi tehniku asimetričnog kriptiranja. Dakle, pošiljatelj i primatelj imaju par ključeva od kojih je jedan tajni, a drugi svima dostupan javni ključ. Klučevi predstavljaju matematičke algoritme koje je izdalo certifikacijsko tijelo

.

.



Svrha digitalnog potpisa je da potvrdi autentičnost sadržaja poruke ili integritet podataka (dokaz da poruka nije promjenjena na putu od pošiljatelja do primatelja ), kao i da osigura garantiranje identiteta pošiljatelja poruke. Osnovu digitalnog potpisa čini sadržaj same poruke. Pošiljatelj primjenom određenih kriptografskih algoritama prvo od svoje poruke koja je proizvoljne dužine stvara zapis fiksne dužine (pr. 512 ili 1024 bita) koji u potpunosti oslikava sadržaj poruke.To prakticno znači da svaka promjena u sadržaju poruke dovodi do promjene potpisa.Ovako dobiven zapis on dalje šifrira svojim tajnim ključem i tako formira digitalni potpis koje se šalje zajedno porukom. Da vidimo kako to funkcionira na našem primjeru.Pero kreira digitalni potpis na osnovu poruke koju želi da pošalje Ani. Šifrira ga svojim tajnim ključem i šalje zajedno sa porukom.Ana po prijemu poruke dešifrira Perin potpis njegovim javnim ključem. Zatim primjenom istog postupka kao i Pero i ona kreira potpis na osnovu poruke koju je primila i upoređuje ga sa primljenim potpisom. Ako su potpisi identični, može biti sigurna da je poruku uistinu poslao Pero (jer je njegovim javnim ključem uspješno dešifrirala potpis) i da je ona stigla do nje nepromjenjena (jer je utvrdila da su potpisi identični).I pored velike sigurnosti koje pruža ova metoda zaštite, i dalje postoji mogućnost prevare. Neko je mogao poslati Ani svoj javni ključ tvrdeći da je Perin, a zatim joj slati poruke za koje bi ona mislila da ih šalje Pero.Rješenje ovog problema pruža upotreba digitalnih certifikata.

## 2.Digitalni certifikati

Ako koristite sistem šifriranja javnim ključem i želite da nekom pošaljete poruku,morate prvo dobiti njegov javni ključ.Međutim, kako možete biti sigurni da je to uistinu njegov ključ? Rješenje ovog problema postiže se upotrebom Digitalnih certifikata. Možemo ih nazvati i digitalnom ličnom kartom, jer oni stvarno to i jesu - digitalna lična karta u syber prostoru, sredstvo kojim ćete vi ili osoba sa kojom komunicirate dokazati identitet na Internetu.Pošto na Internetu nema policije koja bi provjerila vaše podatke i izdala vam ličnu kartu, pojavile su se kompanije koje imaju ulogu ‘treće strane’, - CA(Certificate Authority) čija je uloga da provjere I utvrde nečiji identitet i nakon toga mu izdaju digitalni certifikat.Kako to funkcionira u praksi,npr. Pero podnosi zahtjev za izdavanje certifikata CA kompaniji. CA provjerava njegov identitet na osnovu ličnih dokumenata koje im je prikazao pri podnošenju zahtjeva. Ako je sve u redu Pero im prosleđuje svoj javni ključ za koji CA kreira digitalni potpis i nakon toga izdaje certifikat kojim se potvrđuje da taj javni ključ uistinu pripada Peri.Ako Pero kasnije želi da komunicira sa nekim, pri prvom kontaktu mu šalje digitalni certifikat i svoj javni ključ. S obzirom da svi poznatiji komunikaciski programi u sebi već imaju uključene javne ključeve CA kompanija kojima se vjeruje, primaoc po prijemu ove poruke lako utvrđuje validnost Perinog certifikata.Ovdje je opisan samo jedan dio primjene digitalnih certifikata. Ako želite da na vašoj Web prodavaonici omogućite kupcima plaćanje kreditnim karticama ili prodaju i pružanje povjerljivih informacija, vaš Web server ( server na kome se nalazi vaša prezentacija ) mora imati mogućnosti da radi kao Secure Web server.Neophodan uslov za sve ovo je da zatražite i dobijete digitalni certifikat za vaš server od nekog CA.Digitalni certifikat vašeg servera izdat od strane CA mora da sadrži sljedeće:

* Naziv vaše organizacije
* Dodatne podatke za identifikaciju
* Vaš javni ključ
* Datum do koga važi vaš javni ključ
* Ime CA koji je izdao digitalni certifikat
* Jedinstveni serijski broj

Svi ovi podaci formiraju certifikat koji se na kraju šifrira koristeći tajni ključ CA. Ako korisnik ima povjerenja u CA i ima CA javni ključ, može biti siguran u ispravnost certifikata.Velika je vjerojatnost da Web browser koji korisnik posjeduje I već sadrži javni ključ CA jer su Netscape i Microsoft procjenili kojim se CA može najviše vjerovati, pa su njihove javne ključeve uključili u svoje browsere. Najčešće korišteni standard za digitalne certifikate je X.509.

# 3.Asimetrični algoritmi

# 3.1RSA algoritam

Pod pojomom **algoritma** podrazumevamo precizno opisan postupak za resavanje nekog problema. Obicno je to spisak uputstava ili skup pravila kojima je, korak po korak, opisan postupak za resavanje zadatog problema. Svaki korak algoritma odnosno svako upustvo iz spiska mora da bude definisana operacija. Algoritmi moraju da budu nedvosmisleni i da se zavrsavaju u konacnom broju koraka.

***RSA algoritam* jedan od najkoriscenijih asimetricnih algoritama danas**.

RSA je skracenica koja je nastala od prezimena njegovih tvoraca: Rona **R**ivesta, Adi

**S**hamira i Leonarda **A**dlemana. Svetlost dana ugledao je davne 1977. godine.

U RSA algoritmu kljucnu ulogu imaju veliki prosti brojevi. To su, kao sto znamo, brojevi koji su deljivi samo samim sobom i jedinicom. Prosti brojevi (P i Q) u ovom algoritmu sluze za generisanje javnog i tajnog kljuca i to preko sledecih jednostavnih formula:

Kjavni = P \* Q

Ktajni = (2 \* (P - 1) \* (Q - 1) + 1) / 3

Algoritam kodiranja i dekodiranja sastoji se iz dve formule. Kodiranje:

Mkodirano = (Mizvorno ^ 3) mod Kjavni

Dekodiranje:

Mizvorno = (Mkodirano ^ Ktajni) mod Kjavni Na primer, hocemo da kodiramo rec "MAJA".

Ona u ASCII formi glasi: 77 65 74 65 (M = 77; A = 65; J = 74; A = 65).

Kao dva prosta broja mozemo uzeti, recimo P = 9839 i Q = 22391. U tom slucaju kljucevi koji ce se koristiti bice:

Kjavni = 220305049 i Ktajni = 146848547.

Sada primenimo formule za kodiranje (koristeci samo javni kljuc): (77657465 ^ 3) mod 220305049 = 162621874

Primalac ce primeniti formulu za dekodiranje (koristeci i javni i tajni kljuc): (162621874 ^ 146848547) mod 220305049 = 77657465

Ono sto je pohvalno za ovaj algoritam je njegova jednostavnost, ali i sigurnost. U sledecoj tabeli dato je vreme u odnosu na duzinu kljuca potrebno da kompjuter brzine 1

MIPS iz javnog kljuca izracuna tajni kljuc (na primer, Pentium I kompjuter ima oko 150 MIPS-a).

Za enkripciju fajlova koriste se kljucevi velicine 1024, 2048 ili 4096 bita. Duzina kljuca u bitovima i potrebno vreme:

50 - 3.9 h

100 - 74 god 150 - 10^6 god

1. - 3,8 \* 10^9 god

# 3.2PGP

PGP je hibridni sistem za enkripciju, jer kombinuje i simetricnu i asimetricnu enkripciju. Podaci se pre sifrovanja pakuju, ako je moguce. Ovo je korisno iz dva razloga. Prvi je manja kolicina podataka za prenos. Drugi je dodatna sigurnost, jer se pakovanjem eliminise pojavljivanje slicnih delova u izvornoj datoteci. Mnoge tehnike kriptoanalize iskoriscavaju bas te slicne delove da bi probile zastitu. Naravno, fajlovi koji su ili prekratki za pakovanje ili se ne mogu spakovati dovoljno, ostavljaju se u izvornom obliku. Posle pakovanja, PGP pravi privremeni kljuc, odnosno slucajan broj koji se generise korisnikovim pokretima misa i pritiskanjem tastera, jer su i oni takodje slucajni. Ovaj kljuc ima jednokratnu upotrebu, jer se koristi da bi se podaci sifrovali simetricnom enkripcijom. PGP zatim sifruje **samo** privremeni kljuc asimetricnom enkripcijom i pridruzuje sifrovanim podacima.

Desifrovanje se vrsi suprotnim procesom. Prvo PGP pomocu tajnog kljuca desifruje privremeni kljuc, a njim se onda dalje desifruju podaci.

# 3.3Zasto PGP koristi hibridnu enkripciju?

Razlog je jednostavan: simetricna enkripcija je oko hiljadu puta brza od asimetricne, ali kod simetricne enkripcije postoji problem prenosa kljuca (ako se presretne kljuc, podaci se mogu desifrovati). Kada se ukombinuju ova dva nacina enkripcije, dobija se zeljeni efekat: brza enkripcija sa sigurnim prenosom kljuca. Kljuc se, dakle, prenosi, ali sifrovan tako da ga samo osoba koja ima tajni kljuc moze desifrovati.

Posto PGP koristi asimetricnu enkripciju, to znaci da ima mogucnost digitalnog potpisivanja dokumenata, uz jednu razliku. Umesto da se ceo dokument sifruje tajnim kljucem i od njega generise potpis, to se radi samo na kontrolnom kodu dokumenta (veoma slicno CRC-u). Bilo kakva promena na dokumentu rezultuje promenom u kontrolnom kodu, samim tim potpis vise nije vazeci, a vi znate da je u pitanju falsifikat. Time se izbegava dupliranje duzine dokumenta, jer se potpis ne generise od celog dokumenta.

# 4.Kriptoanaliza

Kriptoanaliza upravo je suprotno od kriptografije. To je nauka koja se bavi razbijanjem sifri, dekodiranjem, zaobilazenjem sistema autentifikacije, uopste provaljivanjem

kriptografskih protokola.Znači kriptoanaliza je naučna disciplina koja proučava postupke otkrivanja otvorenog teksta bez poznavanja ključa, te postupke otkrivanja ključa uz poznavanje otvorenih i/ili kriptiranih tekstova, ili uz poznavanje nekih informacijao otvorenim i/ili kriptiranim tekstovima.. Razlicite tehnike kriptoanalize nazivaju se napadi. Napadi na sigurnost se mogu razdvojiti u pasivne i aktivne napade. Pasivnimnapadom se samo prisluškuje poslana poruka. Pasivni napad je puno težedetektirati nego aktivni napad. Aktivni napad uključuje mijenjanje poruke,maskiranje, ponovno slanje i DoS ('Denial of Service') napade.

### Vrste napada:

* Napad poznatim šifriraniim tekstom: ovaj napad je najteži. Kriptoanalitičarpoznaje samo algoritam kriptiranja i kriptirane tekstove.
* Napad poznatim otvorenim tekstom: za dani kriptirani tekst

kriptoanalitičarpoznaje odgovarajući otvoreni tekst ili njegov dio. Kriptoanalitičar zna algoritam i 1 do N otvorenih i kriptiranih tekstova, ali ne zna ključ.

* Napad odabranim otvorenim tekstom: kriptoanalitičar odabire otvorenitekst i kriptira ga. Ovaj napad omogućuje pronalaženje slabosti ualgoritmu. Kriptoanalitičar zna algoritam, kriptirani tekst i 1 do N odabranihparova otvorenih i kriptiranih tekstova, ali ne zna ključ.
* Napad odabranim kriptiranim tekstom: kriptoanalitičar može odabratikriptirani tekst i na neki način ga dekriptirati i dobiti otvoreni tekst. Takođermože odabrati neki otvoreni tekst po svojoj želji. Kriptoanalitičar zna algoritam, kriptirani tekst i 1 do N navodnih kriptiranih tekstova sa otvorenim tekstovima, ali ne zna ključ.
* Adaptivan napad odabranim otvorenim tekstom: kriptoanalitičar koristinapad odabranim otvorenim tekstom. Rezultati napada se koriste za odabir nekog drugog otvorenog teksta. Ovim načinom moguće je unaprijediti napad. Ovaj napad poznat je pod nazivom "diferencijalna kriptoanaliza". Kriptoanalitičaru je poznat algoritam, kriptirani tekst,dabrani otvoreni tekst sa kriptirani tekstom, te odabrani kriptirani tekst sa otvorenim tekstom.
* Birthday attack: ovaj napad je dobio ime po paradoksu rođendana
* Meet in the Middle: napad je sličan birthday napadu, osim štokriptoanalitičar može provjeriti sjecište između dvaju skupova, a ne moračekati pojavljivanje vrijednosti dvaput u jednom skupu.
* Napad korištenjem srodnih ključeva: u ovom napadu pretpostavlja seznanje o odnosu između ključeva u dva različita kriptiranja. Napad možeotkriti slabosti u postupku generiranja podključeva.
* Djelomično znanje o ključu: napadač posjeduje djelomično znanje o tajnom kljluču (npr. zbog “rupe” u postupku generiranja podključeva). U dobrim kriptosustavima, djelomično znanje o ključu ne bi trebalo olakšati pronalaženje ostatka ključa. Ako nije tako, lakše je izvesti iscrpno pretraživanje.

Prema količini i kvaliteti otkrivenih tajnih informacija može se klasificirati uspjeh kriptoanalize

1. Potpuno probijanje ("Total break") - napadač otkriva ključ.
2. Globalna dedukcija ("Global deduction") - napadač otkriva funkcijski ekvivalent algoritma za kriptiranje i dekriptiranje, ali ne nalazi ključ.
3. Lokalna dedukcija ("Instance (local) deduction") - napadač otkriva dodatne otvorene tekstove (ili kriptirane tekstove), nepoznate od prije.
4. Informacijska dedukcija ("Information deduction") - napadač dobiva Shannon-ove informacije o otvorenim tekstovima (ili kriptiranetekstovima), nepoznatih od prije.
5. Algoritam koji omogućuje razlikovanje ("Distinguishing algorithm") -napadač može razlikovati kriptirane tekst od slučajne permutacije.

# 5.Osnovna pravila zastite

Skoro svi programi za enkripciju umesto brojeva kao kljuca, koriste niz slova i brojeva, tj. lozinku. Svi ovi algoritmi su u velikom stepenu sigurni, bilo da se radi o simetricnim ili asimetricnim, ali postoji sansa da se lozinka otkrije ako se ne pridrzavamo nekih pravila pri njenoj izradi.

### Idealna kombinacija zastite je kombinacija hardver-softver i pridrzavanje dole nevedenog pravila o vise niza slucajnih slova i brojeva prilikom smisljanja lozinke*.*

Evo nekoliko pravila kojih bi trebalo da se pridrzavamo prilikom smisljanja lozinke:

* + - **Idealno je da se za lozinku uzme niz slucajnih slova i brojeva**. Pri tom bi trebalo da se koristi vise od jednog niza slucajnih slova i brojeva. Oakve lozinke mnogi izbegavaju jer ih smatraju teskim za pamcenje i upotrebljavaju reci iz svakodnevnog govora. tom slucaju potrebno je pridrzavati se sledecih pravila:
    - **Ne koristiti reci koje se lako mogu pogoditi**: na primer, godinu rodjenja, devojacko prezime supruge (ili svoje, ako je u pitanju korisnik zenskog pola) , ime deteta, supruznika, roditelja, bliskog rodjaka, psa/macke/kanarinca ili nekog drugog kucnog ljubimca itd.
    - **Trebalo bi koristiti vise od jedne reci**. Izbegavajte upotrebu reci iz recnika u neizmenjenom obliku. Korisno je upotrebiti barem kombinaciju jedne reci sa nekim brojem.
    - **Budite inventivni**. Najbolja lozinka moze biti deo citata iz neke knjige ili neka besmislena recenica.